ANGEMESSENHEITSBESCHLUSS: WIE UNTERNEHMEN DEN DATENTRANSFER NACH GB AUCH IN UNSICHEREN ZEITEN SICHERN KÖNNEN

Clemens Dorner und Dr. Jan Dröge

Seit dem 1. Januar 2021 ist die ambivalente Beziehung zwischen der Europäischen Union (EU) und Großbritannien beendet. Mit dem Brexitabkommen wurde besiegelt, was über Jahre verhandelt wurde. Während die Medien ihr Augenmerk bei den Brexitverhandlungen auf die zukünftige Handelszone und die Zollunion legten, waren Themen wie Datenschutz und zukünftiger Informationsaustausch zwischen beiden Parteien nur Randnotizen.

Was datenschutzrechtliche Belange betrifft, ist Großbritannien seit Jahresbeginn als Drittstaat einzustufen.[1] Rechtsakte Großbritanniens unterfallen nicht mehr der richterlichen Kontrolle der Europäischen Gerichte und die Europäischen Kommission hat ebenfalls keinen Handlungsspielraum mehr.

Für internationale Datentransfers hat dies das Ende der Vermutung eines angemessenen Datenschutzniveaus in Großbritannien zur Folge. Datentransfers zwischen EU und Großbritannien, bzw. zwischen Unternehmen in den jeweiligen Regionen sind nach Maßgabe der Artt. 44 ff DS-GVO zu bewerten.

Nachfolgend werden wir uns insbesondere mit dem Spannungsfeld zwischen den Interessen der EU (Einhaltung der Datenschutz-Grundverordnung (DS-GVO)) und den Interessen Großbritanniens (Innen- und Außenpolitik) auseinandersetzen.

Das Verfallsdatum des Angemessenheitsbeschlusses und die Ankündigung, den UK Data Protection Act zu reformieren, erzeugen ein Spannungsfeld in dessen Mitte besonders Unternehmen die Leidtragenden sein werden.

1. Spannungsfeld EU-Großbritannien

a) Angemessenheitsbeschluss

Am 28. Juni 2021 verabschiedete die EU-Kommission den Angemessenheitsbeschluss für Großbritannien. Dieser ist zunächst auf vier Jahre befristet durch die sogenannte „sunset clause". Hiernach verliert der Angemessenheitsbeschluss nach Ablauf von vier Jahren ohne weiteres Zutun seine Wirkung. In der Laufzeit wird die EU-Kommission die rechtliche Situation beobachten und einschreiten, sollte Großbritannien von dem attestierten Schutzniveau abweichen. Hieraus geht hervor, dass selbst die vier Jahre nicht garantiert sind. Aufgrund aktueller Bestrebungen zur Reformation des britischen Datenschutzrechts kann vermutet werden, dass es nicht zu einer Verlängerung des Angemessenheitsbeschlusses kommt.

a) Britische Politik

Während die EU mit dem Angemessenheitsbeschluss die Spielregeln für den Umgang mit personenbezogenen Daten mit Großbritannien sicherstellen möchte, gibt es zwei politische Entwicklungen im Königreich, die diese Bestrebung torpedieren.

Zum einen hat der Brexit der Wirtschaft auf der Insel erheblichen Schaden zugefügt. Namhafte Unternehmen begannen Ihren Handelsschwerpunkt aus London in die EU zu verlegen. Zur Stärkung Großbritanniens als Wirtschaftsstandort schlug der britische Digitalminister Oliver Dowden eine Vereinfachung des internationalen Datentransfers vor, um die britischen Märkte und Unternehmen für ausländisches Kapital zu öffnen. Erreicht werden soll dies durch ein auf Wirtschaftswachstum und Innovation ausgerich-

[1] Erklärung des EDSA vom 15. Dezember 2020, aktualisiert am 13. Januar 2021.

tetes Datenschutzrecht, internationale Partnerschaften und durch die Beseitigung „unnötiger" Barrieren und Belastungen im internationalen Datentransfers[2].

Beabsichtigt sind unter anderem die nachfolgenden Änderungen:

- eine Liste von vordefinierten berechtigten Interessen, die eine Abwägung der Rechte und Freiheiten des Einzelnen entbehrlich machen soll
- die Aufhebung der Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen und die Einführung alternativer Übermittlungsmechanismen
- eine Änderung des Auskunftsrechts, um für Unternehmen Kosten und Aufwand zu senken
- die Reform des Information Commissioner's Office hin zu einer Institution, die stärker auf Wirtschaftswachstum und Innovation ausgerichtet sein soll

Wenn die britische Regierung alle vorgeschlagenen Änderungen an ihrem Datenschutzrecht durchsetzt, wird sich der Schwerpunkt des Datenschutzes zu einem Gesetz hin verlagern, das stärker auf Unternehmen und Wirtschaftswachstum ausgerichtet ist.

Ein weiterer Faktor ist die enge Zusammenarbeit Großbritanniens mit den Geheimdiensten diverser Staaten außerhalb der EU, zuvorderst den USA. Das sogenannte Five-Eyes-Abkommen zwischen den USA, Großbritannien, Neuseeland, Australien und Kanada dient gegenwärtig der Bekämpfung des internationalen Terrorismus. Zu diesem Zweck wird wohl auch die private Kommunikation überwacht und daraus gewonnene Daten unter den Vertragspartnern ausgetauscht.

Wie der EuGH mit seinem Schrems-II-Urteil feststellte, ist das Datenschutzniveau in den USA dem der EU nicht angemessen. Dies liegt insbesondere an den Zugriffsmöglichkeiten der US-Geheimdienste auf personenbezogene Daten und der fehlenden Möglichkeit, Betroffenenrechte wirksam geltend zu machen. Es gibt also genug Anhaltspunkte, die eine Angemessenheit des Datenschutzniveaus Großbritanniens zukünftig als zweifelhaft erscheinen lassen. Dieser Standpunkt galt zwar schon vor Erlass des Angemessenheitsbeschlusses, würde sich jedoch durch die Umsetzung der geplanten Änderungen im britischen Datenschutzrecht verfestigen und zu einem Wegfall der sicheren Datenübermittlung nach Großbritannien führen. Es ist also nur folgerichtig, ein solches Szenario als mögliche datenschutzrechtliche Zukunft zu betrachten und entsprechende Vorkehrungen im Rahmen unternehmerischer Risikobewertungen zu treffen.

2. Auswirkung auf die Realwirtschaft

Sollte der Angemessenheitsbeschluss frühzeitig aufgehoben oder nicht verlängert werden, stellt sich die Frage: `Was dann?´. Binding Corporate Rules? Standardvertragsklausel? Ausnahmeregelungen? Nachhaltige Lösungen für einen geregelten Datentransfer, wie ihn Unternehmen tagtäglich durchführen, sehen anders aus.

a) Lösungen für Unternehmen?

Ähnlich wie beim Datentransfer mit den USA können wohl viele Unternehmen mit Partnern oder Dienstleistern in Großbritannien nicht auf den Datentransfer verzichten. Für Unternehmen gilt es daher zu klären, wie im Falle des Wegfalls des Angemessenheitsbeschlusses der Datentransfer rechtlich abgesichert werden kann und welches Risiko Unternehmen bereit sind zu tragen.

b) Ausnahmeregelungen Art. 49 DS-GVO

Art. 49 Abs. 1 DS-GVO bieten für die Praxis konkrete Anwendungsfälle, in denen eine Übermittlung an einen Empfänger in einem datenschutzrechtlich unsicheren Drittland erfolgen kann. Der Grundgedanke ist hier nicht, ob die übermittelten Daten in dem Drittland geschützt sind. Art. 49 DS-GVO betrifft vielmehr Fälle, in denen das Risiko in dem Empfängerland bewusst eingegangen wird, sei es aus freier Entscheidung des Betroffenen in Kenntnis der Risiken (Art. 49 Abs. 1 lit. a DS-GVO), weil die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person erforderlich ist (Art. 49 Abs. 1 lit. b und c DS-GVO) oder um überwiegende Interessen durchzusetzen (Art. 49 Abs. 1 lit. d bis f DS-GVO). Die Anwendbarkeit dieser Ausnahmeregelungen dürfte sich für Unternehmen im Alltagsgeschäft jedoch als schwierig gestalten.

Nehmen Sie ein internationales Unternehmen, dessen Verwaltung und Buchhaltung in Großbritannien sitzt. In der Zeit nach Beschluss des

[2] UK unveils post-Brexit global data plans to boost growth, increase trade and improve healthcare - GOV.UK (www.gov.uk)

Austritts aus der EU und vor der Annahme des Angemessenheitsbeschluss musste die Frage der Rechtmäßigkeit eines Datentransfers von teilweise sensiblen Personaldaten nach Großbritannien geprüft werden. Gerade für die Übermittlung von Personaldaten bietet Art. 49 Abs. 1 DS-GVO kaum Möglichkeiten eines gerechtfertigten Datentransfers in der Praxis.

Eine Einwilligung ist jederzeit frei widerrufbar, was ihre Praktikabilität besonders im Beschäftigungskontext deutlich mindert. Der Verantwortliche müsste zum Beispiel klären, wie Daten Beschäftigter übermittelt und verarbeitet werden, die ihre Einwilligungen widerrufen haben. Zudem drängt sich bei Einwilligungen im Beschäftigungsverhältnis die Frage nach der Freiwilligkeit der Einwilligung auf.

Hinsichtlich der Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person muss der Vertrag einen deutlichen Auslandsbezug aufweisen, um eine Datenübermittlung zu rechtfertigen. Anschauliche Beispiele sind Flug- und Hotelbuchungen, die eine Übermittlung personenbezogener Daten in das Empfängerland logischerweise zwingend erforderlich machen.

Anders liegt der Fall etwa bei der Personalverwaltung in einem Drittland. Auch wenn diese Aspekte zentral in einem Drittland verwaltet werden, ist der Beschäftigungsvertrag oft mit dem in der EU ansässigen Arbeitgeber geschlossen. Gehen wir weiter davon aus, dass die Erfüllung des Beschäftigungsvertrags zwar einen gewissen Drittlandbezug aufweist, die Beschäftigung aber im Inland erfolgt, fehlt es an einem deutlichen Drittlandbezug. Zudem dürfte es einem Unternehmen durchaus zumutbar sein, für regelmäßige Datentransfers angemessene Garantien zu schaffen, um die Daten der Mitarbeiter und Kunden zu schützen.[3]

Hinzu kommt die Risikobewertung des verantwortlichen Arbeitgebers. Dieser muss sich bewusst sein, dass eine risikobehaftete Datenübermittlung in ein Drittland ohne Garantien einen Verstoß gegen Art. 32 darstellen kann.

c) Standardvertragsklauseln

Standardvertragsklauseln sind gemäß Art. 46 Abs. 2 lit. c DS-GVO geeignet, den Datentransfer in Drittländer abzusichern. Sie bieten einen flexiblen Anwendungsbereich, da unternehmensinterne Datentransfers sowie jene von Auftragnehmern und Dienstleistern abgesichert werden können.

Die in diesem Jahr verabschiedeten neuen Standardvertragsklauseln mit Modulen für verschiedene Übertragungsszenarien bieten die Möglichkeit, die Standardklauseln individuell anzupassen.

Standardvertragsklauseln galten lange als die einzige Alternative für Unternehmen, um personenbezogene Daten an Empfänger in Großbritannien post Brexit zu übermitteln. So verwies auch der Europäische Datenschutzausschuss in seinen Hinweisen vom 12. Februar 2019[4] auf dieses Instrument im Falle eines ungeregelten Brexits, zuletzt auch in den Hinweisen vom 15. Dezember 2020[5].

Mit der Entscheidung des EuGH in der Rechtssache Schrems II verpflichteten die Richter datenexportierenden Unternehmen auf eine Due-Diligence-Bewertung, um zu überprüfen, ob die Rechte aus der DS-GVO im Zielland nicht beeinträchtigt werden.Die Verantwortung für die Risikobewertung wurde seither bei unterschiedlichen Stellen verortet. Während manche Landesdatenschutzbehörden in Deutschland die Verantwortung für diese umfangreiche Prüfung bei den datenexportierenden Unternehmen sehen (etwas in Berlin), sehen Unternehmensverbände, Unternehmen selbst sowie manche Landesdatenschutzbehörden (zum Beispiel Baden-Württemberg) öffentliche Stellen in der Pflicht.

Bis diese Frage endgültig geklärt ist, bleibt die Pflicht zunächst bei den Datenexporteuren. Der Europäische Datenschutzausschuss riet in seiner Empfehlungen 01/2020 vom 10. November 2020 zu prüfen, ob es in den Gesetzen oder Praktiken des Drittlandes Aspekte gibt, die die Wirksamkeit der angemessenen Garantien der Übermittlungsinstrumente, auf die sich der Datenexporteur stützt, beeinträchtigt werden.[6]

Zur Risikobewertung (Datenübermittlungsfolgenabschätzung, im englischen Transfer Impact Assessment) gehören

- eine systematische Beschreibung des Datentransfers (einschließlich der Verantwortlichkeiten)
- eine Folgenabschätzung für den Datentransfer, welche die Rechtslage im Empfängerland

[3] Kühling/Buchner/Schröder Art. 49 Rn. 19.
[4] Hinweise des EDSA vom 12. Februar 2019 zur Übermittlung von Daten nach der DSGVO im Fall eines ungeregelten Brexit
[5] Hinweise des EDSA vom 15. Dezember zu Datentransfers nach DSGVO nach Ablauf der Übergangsfrist.
[6] Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 10. November 2020.

berücksichtigt und hieraus potenzielle Risiken für betroffene Personen ableitet

- Abhilfemaßnahmen, um das Auftreten der Risiken/Bedrohungen zu mindern (etwa Verschlüsselung der Daten während der Übertragung und im gespeicherten Zustand, Zugriffsbeschränkungen, homomorphe Verschlüsselung)
- ein Abschlussbericht, um der Nachweispflicht aus Art. 5 Abs. 2 DS-GVO gerecht zu werden.
- Sollte der Angemessenheitsbeschluss fallen oder nicht verlängert werden, müssten die Datenexporteure die genannten Prüfungsschritte durchführen. Die Anforderungen an die durch die Datenexporteure zu treffenden zusätzlichen Garantien wären umso höher, da ein unzureichendes Schutzniveau indirekt offiziell bestätigt würde.

Es bietet sich daher an, als Datenexporteuer nicht auf den Angemessenheitsbeschluss zu vertrauen, sondern jetzt schon Maßnahmen zum Schutz der übermittelten personenbezogenen Daten zu treffen. Art. 32 DS-GVO gibt diese Pflicht ohnehin jedem Verantwortlichen auf, womit diese Maßnahmen keineswegs umsonst wären. Sollte der Angemessenheitsbeschluss fallen, könnte ohne weiteres ein Wechsel auf die Standardvertragsklauseln erfolgen, da die Due Diligence bereits vorliegt.

a) Binding Corporate Rules

Die Binding Corporate Rules (BCR) können an den konzernspezifischen Datenschutzoperationen ausgerichtet werden, interne Prozesse abbilden und im Falle von M&A durch den Beitritt des neuen Tochterunternehmens und Anwendung der festgeschriebenen Prozesse erweitert werden. Insoweit bieten BCR eine Alternative für Konzerne und deren Datenschutzorganisation. Parallel zu den Standardvertragsklauseln unterliegen BCR jedoch ebenfalls den Due-Diligence-Anforderungen und müssen darüber hinaus von der zuständigen Aufsichtsbehörde genehmigt werden. Besonders die Genehmigung kann einen erheblichen Zeitverzug bedeuten, da die Aufsichtsbehörden derzeit nicht eindeutig geklärt haben, wie die Schrems-II-Anforderungen in den BCR umgesetzt sein müssen.

Eine wirkliche Lösung für den möglichen Wegfall des Angemessenheitsbeschlusses zwischen der EU und Großbritannien stellen BCR derzeit daher nicht dar.

3. Fazit

Die wirtschaftliche Lage zwingt Großbritannien zu Schritten, die sich auf lange Sicht nachteilig auf das Verhältnis zur EU auswirken könnten. Der Datenschutz ist hiervon genauso betroffen, wie andere Rechtsbereiche. Sollte sich an dem Kurs der britischen Regierung nichts ändern, muss das Ende des Angemessenheitsbeschlusses als eine wahrscheinliche Zukunft in Betracht gezogen werden. Unternehmen sollten deshalb bereits jetzt im Rahmen ihre Rechenschaftspflichten bei ihrer Due Dilligence zu Drittlandtransfers auch Großbritannien in den Fokus nehmen. Nur um sicher zu gehen.

Über die Autoren

Clemens Dorner

ist Rechtsanwalt und Senior Consultant bei der 2B Advice GmbH in Bonn. Er berät international tätige Unternehmen zu allen Fragen des Datenschutzes, ist als externer Datenschutzbeauftragter bestellt und berät in aufsichtsbehördlichen Verfahren. Er ist EuroPriSE Expert für Zertifizierungen und selbst nach IAPP als CIPP/E zertifiziert.

Dr. Jan Dröge LLM.

ist VP Consulting Europe bei der 2B Advice GmbH in Bonn. Er ist als externer Datenschutzbeauftragter für internationale Unternehmen bestellt und betreut globale Datenschutzprojekte zum Aufbau unternehmensinterner Datenschutzorganisationen. Er ist EuroPriSe Expert für Datenschutz-Zertifizierungen und zertifiziert nach IAPP als CIPP/E sowie nach TÜV.

▶ www.2b-advice.com